UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/090,543	03/01/2002	Peter M. Rigstad	3COM-3828.MCD.US.P	5432

7590 12/03/2003

WAGNER, MURABITO & HAO LLP
Two North Market Street
Third Floor
San Jose, CA 95113

EXAMINER	
MOORTHY, ARAVIND K	

ART UNIT	PAPER NUMBER
2131	6

DATE MAILED: 12/03/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/090,543	RIGSTAD ET AL.	
	Examiner	Art Unit	
	Aravind K Moorthy	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 September 2003*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-39* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-39* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *11 June 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) ☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____.
4) ☐ Interview Summary (PTO-413) Paper No(s). _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

1. Claims 1-39 are pending in the application.

2. Claims 1-39 have been rejected.

Response to Amendment

3. The examiner approves the new title to the application.

4. The applicant has overcome the 35 USC § 112 rejections with amendments of claims 1, 7, 11, 22 and 36.

Response to Arguments

5. Applicant's arguments filed 9/8/03 have been fully considered but they are not persuasive.

The applicant argues that Nessett fails to disclose a device having a firewall that allows a communication device to establish a connection to a network even though the communication device does not have a firewall that is accepted by the network. The applicant argues that Nessett fails to disclose a device that allows a communication device to establish a connection to a network provided that the device is in the network.

The examiner respectfully disagrees. The examiner asserts that Nessett teaches the above features as stated in the rejection below.

The applicant argues that the additional references do not teach the above limitations. The examiner asserts that Nessett teaches these features, as stated below, so additional references were not needed to teach the above limitations.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. Claims 1, 4-6, 10, 12, 13, 15-20, 22-24, 32, 33, 36 and 39 rejected under 35 U.S.C. 102(b) as being anticipated by Nessett et al U.S. Patent No. 5,968,176.

As to claims 1, 22 and 36, Nessett discloses a system for providing a firewall to a communication device [abstract]. Nessett discloses a first device comprising a hardware-implemented firewall [column 3, lines 22-27]. Nessett discloses that network devices such as routers, remote access equipment, switches, repeaters and network cards are configured to contribute to the implementation of distributed firewall functions in the network. Nessett discloses that the first device coupled to a host device that is coupled to the communication device for establishing a connection to a network [figure 2]. As shown in figure 2, a repeater **130**, configured as a firewall as discussed above, is coupled to end system **131** (i.e. host device) that is coupled to the NIC communication device. Nessett discloses logic residing in the system to allow the communication device to establish a connection to the network provided the first device is in the system [column 12, lines 10-15]. Nessett discloses that both NIC's and modems provide features for access control. Modems may require a user to provide a password to initiate a connection. Nessett's invention relates to computer network security directed to firewalls. As discussed above, a network card can be implemented as a firewall. The examiner asserts that if the network card were not part of the system, a user would not be able to make a connection to

the network. Nessett discloses that the system is configured to cause data transferred by the communication device to be processed by the firewall [column 11, lines 54-62]. As to the limitation "only if a firewall device comprising a hardware implemented firewall is coupled to a host device" in claim 22, Nessett discloses that the NIC behaves as a pervasive multi layer firewalls [column 11, lines 54-62]. The examiner asserts that if the NIC were not implemented then a device would not be able to connect to the network. Nessett discloses that the first device allows the host device to connect to the network using the communication device that doe not itself have a firewall that is accepted by the network [column 12, lines 57-65]. As to claim 36, the examiner asserts that a NIC is a data interface for receiving and sending data.

As to claim 4, Nessett discloses a server for providing policies to be used by the firewall and that the first device (i.e. NIC) is operable to access the server to receive the policies [column 12, lines 16-21].

As to claim 5, Nessett discloses that the system further comprises a plurality of nodes having a hardware-implemented firewall [figure 1]. The nodes in figure 1 that are hardware-implemented firewalls are the switches, repeaters and NIC's. Nessett discloses that the server is further operable to transfer the policies to the plurality of nodes and that the system comprises a centrally managed network having nodes with hardware implemented firewalls [column 7, lines 22-35].

As to claim 6, Nessett discloses that the logic to allow the system to establish a connection to the network comprises hardware implemented token [column 12, lines 10-16]. Nessett discloses a token card that may require a user to provide a password in order to initiate a connection.

As to claim 10, Nessett discloses logic for preventing login of the host device unless the first device is coupled to the host device [column 12, lines 10-21]. As discussed above, the NIC can be implemented as a firewall. The examiner asserts that if the NIC is not present in the host device, then the host device does not have the capability of login. Without the NIC, a host device would not have means of connecting to a network to login.

As to claim 12, Nessett discloses that the first device is physically coupled to the communication device [figure 2]. As shown in figure 2, repeater **133** is connected to a NIC. Nessett discloses that the data transferred by the communication device to the network is processed by the firewall before it is transferred into the network and the data transferred from the network to the communication device passes through the firewall before it reaches the host device [column 11, lines 54-62].

As to claim 13, Nessett discloses that the physical connection is of the same medium as the network connection (i.e. NIC) [figure 2].

As to claim 15, Nessett discloses that the system further comprises a software driver in the host device and that the driver is operable to pass data that is received by the communication device to the first device to be processed by the firewall [column 6 line 64 to column 7 line 2]. As discussed above, the host device is integrated into the firewall. As disclosed, the software driver is for a NIC card. The software driver of the NIC card makes it operable to pass data that is received by the communication device to the first device to be processed by the firewall.

As to claim 16, Nessett discloses that the software driver is further operable to pass data which is to be transferred by the communication device over the network to the first device to be processed by the firewall, as discussed above.

As to claim 17, Nessett discloses a software component installed above a driver for the communication device, the software component operable to route data for the communication device to the first device [column 4, lines 31-34]. Nessett discloses TCP operating over the Internet Protocol IP. The examiner asserts that TCP operates within an operating system.

As to claim 18, Newton's defines a shim as a piece of software. Microsoft defines a miniport driver as a kernel-mode driver that is specific to a device. As to the limitation "said software component is a shim", TCP is the software component would have been the shim. The miniport driver would have been the driver for the NIC. The examiner asserts that TCP operates within an operating system. The examiner further asserts that an operating system resides above any drivers.

As to claim 19, Nessett discloses a software component installed below a driver for the NIC and that the software component is operable to route data for the communication device to the first device [column 17, lines 41-53].

As to claim 20, Nessett discloses transfer security logic residing on the first device [column 11, lines 54-62]. Nessett discloses that the transfer security logic is for securely transferring data between the first device and a server [figure 2] in the network.

As to claim 23, Nessett discloses that the host device routes the data to the firewall device is to be processed by the hardware-implemented firewall, as discussed above. Microsoft defines the physical layer as being totally hardware-oriented and deals with all aspects of establishing and maintaining a physical link between communicating computers. As disclosed by Nessett, the firewalls all have NIC's. The examiner asserts that the NIC's operate at the physical layer and routes data. Thus, the routing takes place at a physical layer in the data stack.

As to claim 24, Nessett discloses sending policies to the firewall device and that the operation of the hardware implemented firewall is modified [column 7, lines 36-47].

As to claim 32, Nessett discloses transferring data to be transferred over the network by the communication interface device to the firewall device. Nessett discloses processing the data with the hardware-implemented firewall [figure 2]. Nessett discloses that the data is processed by the hardware-implemented firewall before it is transferred over the network connection established via the communication interface device [column 11, lines 54-62].

As to claim 33, Nessett discloses that the host device routes the data to the firewall device is to be processed by the hardware-implemented firewall, as discussed above. Microsoft defines the physical layer as being totally hardware-oriented and deals with all aspects of establishing and maintaining a physical link between communicating computers. As disclosed by Nessett, the firewalls all have NIC's. The examiner asserts that the NIC's operate at the physical layer and routes data. Thus, the routing takes place at a physical layer in the data stack.

As to claim 39, Nessett discloses that the hardware implemented firewall is dedicated to the host device [column 11, lines 25-67].

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 2, 8, 9, 11, 21, 25 and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nessett et al U.S. Patent No. 5,968,176 as applied to claim 1 above, and further in view of Gleichauf et al U.S. Patent No. 6,324,656 B1.

As to claim 2, Nessett does not teach logic for checking integrity of software components in the system.

Gleichauf teaches logic for checking integrity of software components in the system. Gleichauf teaches that network devices are scanned for the potential vulnerabilities inherent to the services and the operating system of each device [column 5, lines 41-45].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Nessett so that the computer implemented firewall would have performed a scan for the potential vulnerabilities to the services and the operating system for each device.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Nessett by the teaching of Gleichauf is that each device connected to the network can identified and the appropriate vulnerabilities can be assessed [column 2, lines 51-54].

As to claim 8, Nessett does not teach an alert log for logging possible breaches detected by the system.

Gleichauf teaches an alert log for logging possible breaches detected by the system. Gleichauf teaches database **26** that can include potential vulnerabilities identified by the NVA engine **20** [column 4, lines 47-49].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Nessett so that the computer implemented firewall would have performed a scan for the potential vulnerabilities and stored the potential vulnerabilities in a database.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Nessett by the teaching of Gleichauf is that once identified, potential vulnerabilities can be confirmed [column 2, lines 55-56].

As to claim 9, Gleichauf teaches a configuration integrity checker (i.e. NVA engine **20**) for checking integrity of software components (i.e. operating system) in the system, wherein the possible breach is detected by the configuration integrity checker [Gleichauf column 5, lines 41-45].

As to claim 11, Nessett does not teach a configuration integrity checker that checks the integrity of software components residing in the host device.

Gleichauf teaches a configuration integrity checker that checks the integrity of software components residing in the host device. Gleichauf teaches that network devices are scanned for the potential vulnerabilities inherent to the services and the operating system of each device [column 5, lines 41-45].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Nessett so that one of the computer implemented firewalls would have performed a scan for the potential vulnerabilities to the services and the operating system for the host device.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Nessett by the teaching of Gleichauf is that each device connected to the network can identified and the appropriate vulnerabilities can be assessed [column 2, lines 51-54].

As to claim 21, Nessett teaches server for providing policies to be used by the firewall [abstract].

Nessett does not teach a configuration integrity checker for checking integrity of software components in the system. Nessett does not teach an alert log for logging possible security breaches detected by the system. Nessett does not teach a server for providing policies to be used by the firewall.

Gleichauf teaches a configuration integrity checker for checking integrity of software components in the system. Gleichauf combination teaches a configuration integrity checker (i.e. NVA engine **20**) for checking integrity of software components (i.e. operating system) in the system. Gleichauf teaches that the possible breach was detected by the configuration integrity checker [column 5, lines 41-45]. Gleichauf teaches an alert log for logging possible breaches detected by the system. Gleichauf teaches database **26** that can include potential vulnerabilities identified by the NVA engine **20** [column 4, lines 47-49]. Gleichauf teaches an alert log for

logging possible security breaches detected by the system. Gleichauf teaches database **26** that can include potential vulnerabilities identified by the NVA engine **20** [column 4, lines 47-49].

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Nessett so that an NVA engine would have been included on the computer that the firewall resides. The NVA would have scanned the software components of the devices on the network and recorded a log for possible security breaches. The server of Nessett would have provided the policies for the NVA engine.

The motivation to have modified Nessett by the teaching of Gleichauf is that each device connected to the network can identified and the appropriate vulnerabilities can be assessed [column 2, lines 51-54].

As to claim 25, Nessett does not teach logic for checking integrity of software components on the host device.

Gleichauf teaches logic for checking integrity of software components in the system. Gleichauf teaches that network devices are scanned for the potential vulnerabilities inherent to the services and the operating system of each device [column 5, lines 41-45].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Nessett so that the computer implemented firewall would have performed a scan for the potential vulnerabilities to the services and the operating system for the host device.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Nessett by the teaching of Gleichauf is that each device

connected to the network can identified and the appropriate vulnerabilities can be assessed [column 2, lines 51-54].

As to claim 34, Nessett teaches server for providing policies to be used by the firewall [abstract].

Nessett does not teach a configuration integrity checker for checking integrity of software components on the host device. Nessett does not teach an alert log for logging possible security breaches detected by the system. Nessett does not teach a server for providing policies to be used by the firewall.

Gleichauf teaches a configuration integrity checker for checking integrity of software components in the system. Gleichauf combination teaches a configuration integrity checker (i.e. NVA engine **20**) for checking integrity of software components (i.e. operating system) in the system. Gleichauf teaches that the possible breach was detected by the configuration integrity checker [column 5, lines 41-45]. Gleichauf teaches an alert log for logging possible breaches detected by the system. Gleichauf teaches database **26** that can include potential vulnerabilities identified by the NVA engine **20** [column 4, lines 47-49]. Gleichauf teaches an alert log for logging possible security breaches detected by the system. Gleichauf teaches database **26** that can include potential vulnerabilities identified by the NVA engine **20** [column 4, lines 47-49].

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Nessett so that an NVA engine would have been included on the computer that the firewall resides. The NVA would have scanned the software components of the host device on the network and recorded a log for possible security breaches. The server of Nessett would have provided the policies for the NVA engine.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Nessett by the teaching of Gleichauf is that each device connected to the network can identified and the appropriate vulnerabilities can be assessed [column 2, lines 51-54].

8. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Nessett et al U.S. Patent No. 5,968,176 and Gleichauf et al U.S. Patent No. 6,324,656 B1 as applied to claim 2 above, and further in view of Servi U.S. Patent No. 5,278,904.

As to claim 3, the Nessett-Gleichauf combination teaches a server for providing policies to be used by the firewall [figure 1].

The Nessett-Gleichauf combination does not teach that the first device further comprises stored values to access the server to receive the policies.

Servi teaches a stored password on a requesting node to access protected resources on a server node [column 1, lines 55-63].

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the Nessett-Gleichauf combination so that any of the firewall devices would have been authenticated by a stored password to receive policies from the security policy server.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Nessett-Gleichauf combination by the teaching of Servi is that this provides a method for reliable identification of a device attempting access to protected resources by a remote verifier using reduced communications [column 1, lines 45-47].

9. Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Nessett et al U.S. Patent No. 5,968,176 as applied to claim 1 above, and further in view of Servi U.S. Patent No. 5,278,904.

As to claim 7, Nessett teaches that the second device is coupled to the first device.

Nessett does not teach a second device having stored thereon data needed to establish the connection to the network. Nessett does not teach logic to allow the system to establish the connection and is operable to access the data to assure the first device must be in the system to establish the connection to the network via the communication device

Servi teaches a stored password on a requesting node to access protected resources on a server node [column 1, lines 55-63].

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Nessett so that any of the firewall devices would have been authenticated by a stored password to receive policies from the security policy server. The password would have been stored data used to establish the connection to the network.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Nessett is that this provides a method for reliable identification of a device attempting access to protected resources by a remote verifier using reduced communications [column 1, lines 45-47].

10. Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over Nessett et al U.S. Patent No. 5,968,176 as applied to claim 1 above, and further in view of Dempsey et al U.S. Patent No. 5,826,048.

As to claim 14, Nessett does not teach that the physical connection comprises an MPCI (Mini Peripheral Component Interconnect) adapter to couple the first device to the communication device.

Dempsey teaches a MPCI interface for connecting a PCI bus to one or more external devices [column 2, lines 43-45].

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Nessett so that the MPCI interface would have connected the firewall to the NIC.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Nessett by the teaching of Dempsey is that it reduces the number of signals required in implementing a PCI compliant interface by multiplexing and subsequently de-multiplexing signals. It also can be used to interface non-PCI devices and bus, and can be adapted or modified to reduce the number of pins/signals associated with these devices and buses [column 3, lines 51-58].

11. Claim 26 is rejected under 35 U.S.C. 103(a) as being unpatentable over Nessett et al U.S. Patent No. 5,968,176 and Gleichauf et al U.S. Patent No. 6,324,656 B1 as applied to claim 25 above, and further in view of Watson et al U.S. Patent No. 5,475,839.

As to claim 26, the Nessett-Gleichauf combination does not teach that the configuration integrity check is performed before the network connection is allowed and the connection is allowed only if the configuration integrity check passes.

Watson teaches that tests are performed prior to or during the boot operation in order to determine whether selected programs and/or data files have been corrupted [column 3, lines 60-63]. The examiner asserts that the boot operation takes place before a network connection takes place.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Nessett-Gleichauf combination so that tests are performed on the host device prior to or during the boot operation in order to determine if any data files have been corrupted. If anything is corrupted the boot process would have been interrupted.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Nessett-Gleichauf combination by the teaching of Watson is that allows the user to boot the system from a known, uncorrupted set of files in the event the system is corrupted [column 3 line 67 to column 4 line 3].

12. Claims 27 and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nessett et al U.S. Patent No. 5,968,176 and Gleichauf et al U.S. Patent No. 6,324,656 B1 as applied to claim 25 above, and further in view of Fischer U.S. Patent No. 5,475,826.

As to claim 27, the Nessett-Gleichauf combination does not teach that performing a hash on the software component to produce a hash value and comparing the hash value with a stored hash value to perform the configuration integrity check.

Fischer teaches it is well known that file integrity is protected by taking a one-way hash (e.g., by using MD5 or the secure hash algorithm SHA) over the contents of the file. By implementing and checking a currently computed hash value, with a previously stored hash value, correct file integrity assures the threat of malicious tampering (or even accidental external modification) can be detected--thereby improving the reliability and security of ultimate results. Assuming it is stored in a way that preserves its own integrity, the file hash can be used to insure that the entire file has not been damaged or deliberately tampered [column 1, lines 37-47].

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Nessett-Gleichauf combination so that a hash on the software component is done to produce a hash value and compared with a stored hash value on the firewall to perform the configuration integrity check.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Nessett-Gleichauf combination by the teaching of Fischer is that massive re-computation for each file alteration, long periods in which the file is in jeopardy of being considered "invalid" if the application or system is abruptly terminated,

additional storage space for a hash (or MAC) for each record, and the ability of an adversary to substitute stale records because the integrity of the entire file, and the inter-relationship of all records is maintained encapsulated in a single file HASH value which changes as each file update is performed [column 3, lines 48-57].

As to claim 28, the Nessett-Gleichauf-Fischer combination that the stored hash value resides on the firewall device, as discussed above.

13. Claims 29, 30 and 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nessett et al U.S. Patent No. 5,968,176 and Gleichauf et al U.S. Patent No. 6,324,656 B1 as applied to claim 25 and 34 above, and further in view of Daniel et al U.S. Patent No. 4,823,345.

As to claim 29, the Nessett-Gleichauf combination does not teach sending an alert if the configuration integrity check fails.

Daniel teaches a generic alert code generation and identification method and apparatus that can identify a particular generic alert [column 2, lines 15-20].

It would have been obvious to a person having ordinary skill in the art at the time the invention was to have modified the Nessett-Gleichauf combination so that an alert is generated if the integrity check fails.

The examiner asserts that the motivation to have modified the Nessett-Gleichauf combination by the teaching of Fischer is that it is obvious that an administrator or user would want an alert to know when something is corrupt in a network device.

As to claim 30, the Nessett-Gleichauf –Fischer combination teaches storing an alert if the configuration integrity check fails [Fischer column 3, lines 44-59].

As to claim 35, the Nessett-Gleichauf combination does not teach sending an alert if the configuration integrity check fails.

Daniel teaches a generic alert code generation and identification method and apparatus that can identify a particular generic alert [column 2, lines 15-20].

It would have been obvious to a person having ordinary skill in the art at the time the invention was to have modified the Nessett-Gleichauf combination so that an alert is generated if the integrity check fails.

The examiner asserts that the motivation to have modified the Nessett-Gleichauf combination by the teaching of Fischer is that it is obvious that an administrator or user would want an alert to know when something is corrupt in a network device.

14. Claims 31 is rejected under 35 U.S.C. 103(a) as being unpatentable over Nessett et al U.S. Patent No. 5,968,176 and Gleichauf et al U.S. Patent No. 6,324,656 B1 as applied to claim 25 above, and further in view of Uceda-Sosa et al U.S. Patent No. 6,496,840 B1.

As to claim 31, the Nessett-Gleichauf combination teaches that host device treats the communication interface device as the firewall device and vice versa, as discussed above. The Nessett-Gleichauf combination teaches that the communication interface device transferring data received from the network in to the firewall device, wherein the firewall device processes the data with the hardware implemented firewall, as discussed above.

The Nessett-Gleichauf combination does not teach swapping resource spaces in the host device that are reserved for the communication interface device and the firewall device.

Uceda-Sosa teaches executing a current modification request on one or more resources of a backup resource group; and atomically swapping the modified backup resource group and a

current resource group, such that the modified backup resource group becomes the current resource group [column 1, lines 34-45].

It would have been obvious to a person having ordinary skill in the art at the time the invention was to have modified the Nessett-Gleichauf combination so that the resources would have been swapped in the host device that was reserved for the communication device and the firewall device so that the NIC would have been the firewall.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Nessett-Gleichauf combination by the teaching of Uceda-Sosa is that it provides a platform independent, application-level technique that provides all-or-nothing semantics at the atomicity level of the underlying operating system, by providing a fixed-size naming scheme and a technique that determines which version of the resource group is the current version [column 5, lines 8-18].

15. Claims 37 is rejected under 35 U.S.C. 103(a) as being unpatentable over Nessett et al U.S. Patent No. 5,968,176 as applied to claim 36 above, and further in view of Fischer U.S. Patent No. 5,475,826.

As to claim 37, Nessett does not teach logic for performing a configuration integrity check of software component. Nessett does not teach that the logic is operable to produce a numeric value that results from the check. Nessett does not teach a stored value for each software component to be checked for integrity. Nessett does not teach logic to compare the produced value with the stored value.

Fischer teaches it is well known that file integrity is protected by taking a one-way hash (e.g., by using MD5 or the secure hash algorithm SHA) over the contents of the file. By

implementing and checking a currently computed hash value, with a previously stored hash value, correct file integrity assures the threat of malicious tampering (or even accidental external modification) can be detected--thereby improving the reliability and security of ultimate results. Assuming it is stored in a way that preserves its own integrity, the file hash can be used to insure that the entire file has not been damaged or deliberately tampered [column 1, lines 37-47].

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Nessett so that a hash on the software component is done to produce a hash value and compared with a stored hash value on the firewall to perform the configuration integrity check.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Nessett by the teaching of Fischer is that massive re-computation for each file alteration, long periods in which the file is in jeopardy of being considered "invalid" if the application or system is abruptly terminated, additional storage space for a hash (or MAC) for each record, and the ability of an adversary to substitute stale records because the integrity of the entire file, and the inter-relationship of all records is maintained encapsulated in a single file HASH value which changes as each file update is performed [column 3, lines 48-57].

16. Claim 38 is rejected under 35 U.S.C. 103(a) as being unpatentable over Nessett et al U.S. Patent No. 5,968,176 as applied to claim 36 above, and further in view of Servi U.S. Patent No. 5,278,904.

As to claim 38, Nessett teaches that a user would have to provide proof that he is authorized to initiate a connection [column 12, lines 10-15]

Nessett does not teach that the first logic comprises stored values to be used in an authentication process during establishment of the network connection.

Servi teaches a stored password on a requesting node to access protected resources on a server node [column 1, lines 55-63].

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Nessett so that any of the firewall devices would have been authenticated by a stored password to establish a network connection.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Nessett is that this provides a method for reliable identification of a device attempting access to protected resources by a remote verifier using reduced communications [column 1, lines 45-47].

Conclusion

17. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K Moorthy whose telephone number is 703-305-1373. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-746-7239.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-1373.

Aravind K Moorthy
November 21, 2003

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100